AB **SCIEX**

Considerations When Validating Your Analyst® Software

INTRODUCTION

The purpose of this white paper is to assist users in validating their Analyst® Software.

WHAT IS VALIDATION?

The FDA considers software validation to be "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled."[1] Note the terms "objective evidence" and "particular requirements." Confirmation of conformity to user needs and intended uses is obtained by comparing actual system performance to pre-determined requirements.

Validation, in the context of government regulation, is distinct from hardware Installation Qualification/Operational Qualification/Instrument Performance Verification (IQ/OQ/IPV).

The purpose of the validation project is to document that the decisions made regarding the system have been properly designed, documented, executed, and verified. It is important to demonstrate that actions were properly planned, that the actions were executed according to the plan, and that the correct records have been kept.

WHO IS RESPONSIBLE FOR VALIDATION?

Validation is the responsibility of the business process owner. Often, this is the Good Lab Practice (GLP) laboratory manager. However, the Quality Assurance Unit also has a role to play in validation. Ultimately, upper management provides the impetus and resources for validation and must "accept" that the system is validated. The laboratory manager is a key member of the validation team, which also includes representatives from all validation stakeholders.

While an organization can utilize third parties to design and perform the validation, the responsibility for validation and the maintenance of a validated state cannot be delegated.

TO VALIDATE OR NOT?

The decision to validate, what to validate, and how, is an exercise in risk management. The regulatory environment (e.g., GLP, GMP, etc.), the specific application of the system (e.g., metabolic studies in support of a new drug application, quality control in drug manufacture), and the degree of risk-tolerance of the organization, will determine how much effort to expend on the validation.

THE COST OF COMPLIANCE VS. THE COST OF NON-COMPLIANCE

The cost of compliance may be tens or hundreds of thousands of dollars. The cost of noncompliance can be measured in tens or hundreds of millions of dollars.

The decision to forego validation means accepting the risk of noncompliance. The decision to validate key sub-systems thoroughly, and other functions minimally, does not eliminate risk, but it does reduce it to manageable levels, while controlling validation effort and expense. The decision to fully validate all components of a system moves farther toward risk avoidance, but is more expensive.

PROSPECTIVE VS. RETROSPECTIVE VALIDATION

Ideally, the validation process should begin at the earliest stages of system acquisition. It is not possible to select a computerized system without understanding the needs of stakeholders and regulation requirements. To ensure that a system meets its intended needs, it is important to have a clear definition of those needs.

In practice, it is sometimes necessary to validate an existing system. In this case, it is still necessary to clearly state the requirements of the system and to verify that those requirements are met.

The validation process continues throughout the lifecycle of the system. Changes to the system will be necessary as is the need to confirm that the system remains validated in the face of those changes. Planning for the ultimate retirement of the system is also part of the validation process.

RULES AND REGULATIONS

Rules and regulations for laboratory systems can be found in 21 CFR 211 (Good Manufacturing Practice), 21 CFR 58 (Good Laboratory Practice), 21 CFR 820 (Quality System Regulation for Medical Devices), 21 CFR Part 11 (Electronic Records and Electronic Signatures), as well as several others. An analysis of the relevant regulations is beyond the scope of this paper. The thrust of the regulations can be summarized as follows: Validation is a required activity that should document that the system is secure, reliable, and fit for its intended purpose, and continues to be so throughout its operation.

CONTROLS: TECHNICAL AND PROCEDURAL

To satisfy regulations, it is necessary to place controls in the system. Controls can be of two types:

1) Technical controls are enforced through hardware and software. For example, the door to a lab will probably have an electronic lock. A user must identify themselves to the lock in order to open the door by entering a pass code, presenting an electronic identification such as a badge, or through a biometric identify verification. Technical controls reduce human effort through automation and reduce the incidence of human error.

2) Procedural controls are equally necessary. For instance, the lab should have a Standard Operating Procedure (SOP) describing the assignment, distribution, and maintenance of electronic passwords and badges. If an employee lends her badge to another employee who in turn uses it to access a restricted area, the technical control at the entry door is compromised. Procedural controls must ensure that each employee has a unique identification, and that the identification remains in the sole possession of the employee to whom it was assigned.

STANDARD OPERATING PROCEDURES (SOPs)

SOPs are necessary, and are a major part of the procedural controls of the system. Some requirements, such as training, cannot be satisfied through technical controls, but must be satisfied through procedural controls. Some important SOPs include issuance and control of usernames and passwords, training procedures, change control procedures, documentation maintenance procedures, backup and restoration of data, and archival and retrieval of data. It is also worthwhile to document your company's software validation procedures in an SOP.

CHANGE CONTROL

Change is inherent in any computerized system. As new requirements are identified, errors found, and procedures revised, changes to the system will be necessary. It is essential that changes to a validated system be carefully controlled. Any change contemplated should be documented, analyzed, and tested. It is not adequate to test only the change. A change to one subsystem might affect other, seemingly unrelated, parts of the system. Minimally, a change should: 1) be requested in writing via a Change Request, 2) be analyzed and approved by the technical resources involved, 3) be the subject of a risk assessment, and 4) be approved by the Quality Assurance Unit.

The Change Control policy should be documented in an SOP.

Failure to control change will result in a system that is not fully validated and expose the business to the risk of non-compliance.

SOFTWARE CATEGORIES

The GAMP® Good Practice Guide: Validation of Laboratory Computerized Systems classifies computer software in five categories and computer hardware in two catergories[3]. Analyst® Software is a category IV, commercial off-the-shelf (Configurable COTS) application. Analyst Software supports the use of custom software, in the form of report templates and scripts. Analyst Software is configurable because it accommodates the storage and persistence of user names, passwords, customized audit trails, and instrument configuration. The effort required to validate a configurable system such as Analyst Software, is greater than that required to validate operating systems, firmware, and standard software. Custom or bespoke software requires even greater validation effort.

THE USER REQUIREMENTS SPECIFICATION

Prior to acquiring a computerized system, it is necessary to objectively state the requirements that the system is intended to fulfill. This is done through a document called a User Requirements Specification (URS). The URS states the criteria that will be used to judge the overall suitability of the system. The URS must address Analyst Software technical controls, procedural controls, capacities, accuracy, security, fault tolerance, physical environment, and training requirements, among others. It is critical that the URS be a complete statement of the needs and objectives of the acquiring organization. A typical URS will contain up to several hundred unique requirements.

THE VALIDATION PLAN

The Validation Plan is a key strategic planning document that describes the entire validation effort and covers the system life cycle from inception to retirement. The regulations place great emphasis on the Validation Plan, because it is the key to controlling the validation project. At a minimum, the Validation Plan should describe the scope of the validation project, the work to be done, and the schedule of activities. It should also identify the individuals responsible for planning, execution, testing, and approval. A prototype for a Validation Plan can be found in reference 5.

CONFIGURATION SPECIFICATIONS

Analyst Software is configurable. The software is used to operate the mass spectrometer and is adaptable to variations in instrument and peripheral equipment setup, security, and data processing. It is necessary to document the intended configuration and document that the actual configuration matches that configuration. Some examples of the Analyst Software features that are addressed in the Configuration Specification are: security and user roles, audit trail settings, equipment configuration, and quantitation settings.

When changes to the Analyst Software configuration are required, they must be evaluated and approved according to the written Change Control policy.

PQ TESTING

The qualification of Analyst® Software can be separated into four phases: 1) Design Qualification (DQ), 2) Installation Qualification (IQ), 3) Operational Qualification (OQ), and 4) Performance Qualification (PQ). It is not always clear in which phase a particular requirement or test belongs. Hardware IQ and OQ will normally be performed on-site by a qualified AB SCIEX field service engineer, as well as the software IQ and OQ. For GAMP® category four software, such as Analyst Software, the DQ is performed by AB SCIEX, the vendor. PQ is generally the focus of a validation effort.

DQ should be verified by performing a vendor audit. AB SCIEX provides a standard postal audit description, that addresses the common elements of a vendor audit. The vendor audit identifies the quality procedures in place, such as ISO 9001 (which AB SCIEX implements) as well as the development and verification methodology.

PQ Testing usually involves the execution of a pre-defined set of actions. A PQ Test Script contains the acceptance criteria, a list of actions, the expected result of each action, the overall results of the test, and the procedure for collecting objective evidence. Good test scripts will specifically reference each applicable requirement. A single test script might address several requirements and range from a small number of steps up to several hundred. Normally, test scripts are organized around a specific range of functionality such as security or data acquisition.

Test scripts must be carefully designed and should include both positive and negative tests. For example, a test for password acceptance will include procedures to verify the result of entering a valid password as well as the result of entering an invalid password.

If a test step fails, then a Deviation Report is required. The Deviation Report should identify the nature of the deviation, the test script or procedure where the deviation occurred, proposed corrective action, and responsibility for implementation and verification.

OBJECTIVE EVIDENCE

Regulations require that objective evidence of each test procedure and its result be retained. Such evidence may be in the form of printed documents, screen shots, result data files, etc. This is particularly true for technical controls. The point is not simply to produce a mountain of documentation, but rather to demonstrate that the software satisfies each requirement.

TRACEABILITY MATRIX

The Traceability Matrix (TM) shows the relationship between each user requirement and a corresponding test script (in the case of technical controls) or SOP (for procedural controls). The TM makes it possible to confirm that each user requirement has been addressed and satisfied by the validation procedure. The TM also records the results of tests performed, deviations encountered, and comments. It is not sufficient to document each test script because a single test script might address several requirements. The organization of the TM should be by requirement, so that it is clear that each and every requirement is verified by testing.

21 CFR PART 11 COMPLIANCE

Analyst Software supports compliance with 21 CFR Part 11, Electronic Records; Electronic Signatures[2]. Part 11 regulates the security, reliability and integrity of laboratory data, and the security and integrity of electronic signatures. The predicate rules contain relatively few signature requirements. Where signatures are required, such as in a data audit trail, Part 11 defines how an electronic signature must be derived and the meaning of the electronic signature. Many Part 11 requirements will be met with a combination of technical and procedural controls.

To help support compliance with Part 11, it is important that appropriate SOPs are in place and the software has been configured correctly. Documents are available that describe the important considerations and necessities of configuration.

QUALITY ASSURANCE UNIT

The Quality Assurance Unit (QA or QC department) must be actively engaged in the validation effort. Management's certification of validation depends on the recommendation of QA. Each document prepared in the course of the validation project should be reviewed and approved by QA. In addition, the resulting documentation set should be reviewed for completeness and consistency. Finally, the QA department must submit recommendations to management regarding the release of the system for use. The best way to ensure that the QA department can recommend the release of the system is to include them in the validation effort throughout the lifecycle.

IMPORTANT DOCUMENTS

The validation documentation set should contain at least the following documents:

• User Requirements Specification

• Configuration Specification

• PQ Test Plan

• Test Cases

• Deviation Reports

• Quantitation Validation Report (if applicable)

• Traceability Matrix

• Validation Summary Report

• Quality Assurance Review and Recommendation

• Validation Certification

PLANNING FOR MAINTENANCE OF THE VALIDATED STATE

Analyst Software validation is not a one-off process. The validation effort should encompass the entire system lifecycle, from inception to retirement. The most important tool for maintaining a system in its validated state is the Change Control Procedure. By carefully following a pre-defined plan for evaluating and approving changes to the system, the physical environment, and the procedural environment, a system can be maintained in a validated state over time.

CONCLUSION

Analyst Software validation need not be an onerous undertaking. By adopting the best practices prescribed by regulatory bodies and professional societies, validation can be performed efficiently. As important as regulatory compliance, the processes and business objectives of the organization are enhanced by proper validation.

For more information on AB SCIEX Professional Services, contact your local AB SCIEX Sales representative or email: **complianceservices@absciex.com**

REFERENCES

1. General Principles of Software Validation; Final Guidance for Industry and FDA Staff. U.S. Department of Health and Human Services, Food and Drug Administration, 2002.

2. Draft Guidance for Industry: 21 CFR Part 11; Electronic Records; Electronic Signatures Validation (WITHDRAWN). U.S. Department of Health and Human Services, Food and Drug Administration, 2001.

3. GAMP® Good Process Guide: Validation of Laboratory Computerized Systems. International Society for Pharmaceutical Engineering, 2005.

4. The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture – GAMP® 4, International Society for Pharmaceutical Engineering, 2001.

5. IEEE Standard for Software Verification and Validation (IEEE Standard 1012), The Institute of Electrical and Electronic Engineers, 2005.

CONTACT US

To learn more about the AB SCIEX Analyst® Software Validation Service, contact your local AB SCIEX Sales representative or email: **complianceservices@absciex.com**